REMARKS

Claims 1-10, 13-20, 22-23, 25-30, 33-38, 40-47 and 50-57 are pending in the present application. In the above amendments, claims 1, 3, 5-10, 13, 19, 22-23, 25-27, 29-30, 33-37, 40-44, 46-47 and 50-57 have been amended, and claims 11, 12, 21, 24, 31, 32, 39, 48 and 49 have been canceled.

Applicants respectfully respond to this Office Action.

Claim Rejections – 35 USC § 103(a)

Claims 1-10, 13-20, 22-23, 25-30, 33-38, 40-47 and 50-57 were rejected under 35 U.S.C. §103(a) as being unpatentable over Ekdahl et al., "SNOW – a new stream cipher", Nov. 2001 (hereinafter referred to as the Ekdahl publication) in view of U.S. Patent No. 6,560,212 B1 to Prasad et al.

The rejection of independent claim 1 as being unpatentable over the Ekdahl publication in view of the Prasad patent is respectfully traversed. Claim 1, as amended, recites, "A method of generating a key stream comprising: selecting input words from a first array of words, wherein each input word comprises two or more bytes; mixing at least two input words to generate primary mixed words; performing a byte-wise substitution of at least one byte of each of the primary mixed words to generate respective primary intermediate words; mixing at least two bytes of each of the primary intermediate words to generate respective secondary intermediate words; mixing at least two secondary intermediate words to generate output words; selecting mask words from a second array of words; and combining the output words with the mask words to generate a key stream block for the key stream; wherein the first and second arrays are finite." The amendments to claim 1 are supported by Figure 2, paragraph [0041], and claims 11, 12, 21 and 24, of the original specification.

In the Office Action, with respect to now canceled claims 11, 12, 21 and 24, which claims recited particular features some of which are now recited in a similar manner in amended claim 1, the Examiner asserted, "[a]s per claims 11-26, 31-36 and 48-53 Ekdahl further teaches the method wherein each value comprises of one or more words and wherein each word comprises two or more bytes (figure 1, 2 and section 2, a description of SNOW)." See, Office Action, page

6. Applicants respectfully submit that the Examiner has not made a prima facie showing that the cited art discloses mixing at least two input words, performing a byte-wise substitution, mixing at least two bytes of the primary intermediate words, and mixing at least two secondary intermediate words, as recited in claim 1.

Accordingly, the rejection of claim 1, as being unpatentable over the Ekdahl publication in view of the Prasad patent, should be withdrawn.

It is respectfully submitted that dependent claims 2-10, 13-20, 22-23, 25-26 and 54 are at least allowable for the reasons given above in relation to independent claim 1. Further, of particular note, claim 13 recites "performing a nonlinear substitution", claim 19 recites "a minimum distance separable matrix multiplication", and claims 22 and 25 recite "modular arithmetic", which features are not disclosed by the Ekdahl publication and the Prasad patent, taken singly or in combination.

Claims 27-30, 33-38, 40-47, 50-53 and 55-57 are apparatus and computer readable medium claims having features defined by language similar to that of method claims 1-10, 13-20, 22-23, 25-26 and 54. Accordingly, for the reasons recited above with respect to claims 1-10, 13-20, 22-23, 25-26 and 54, claims 27-30, 33-38, 40-47, 50-53 and 55-57 define patentable advances over the Ekdahl publication and the Prasad patent, and the rejections of claims 27-30, 33-38, 40-47, 50-53 and 55-57 should be withdrawn.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicants submit that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: **October 29, 2009**

By:
Won Tae C. Kim, Reg. # 40,457
(858) 651 - 6295

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502